迪普科技 2018 年 6 月

信息安全研究月报

杭州迪普科技股份有限公司

Hangzhou DPTech Technologies Co.，Ltd.

目 录

一、 安全漏洞态势

2018 年 6 月份新增安全漏洞 177 个。比上月增加了 59 个，与前 5 个月平均数量相比，安全漏洞数量大幅减少。本月新增的漏洞中，高危漏洞 58 个，中危漏洞 115 个，低危漏洞 4 个，同比 2017 年 6 月（漏洞总数 825 个）减少 78.55%。表 1-1 为 2018 年 1 月-2018 年 6 月漏洞危险等级统计。

表 1-1 2018 年 1 月-2018 年 6 月漏洞危险等级统计

	一月	二月	三月	四月	五月	六月
高危	**237**	**367**	**144**	**436**	**48**	**58**
中危	**438**	**502**	**277**	**313**	**65**	**115**
低危	**121**	**112**	**52**	**56**	**5**	**4**
总数	**796**	**981**	**473**	**805**	**118**	**177**

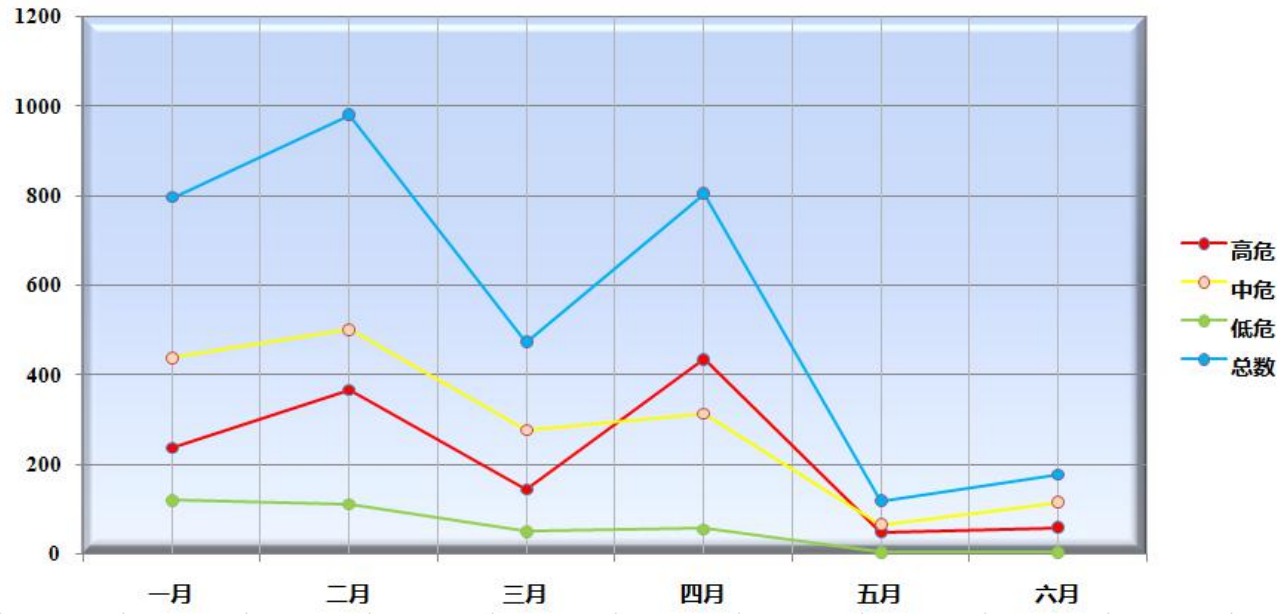

图 1-1 2018 年 1 月-2018 年 6 月漏洞新增数量趋势

二、 漏洞类型分布

2018 年 6 月份新增的漏洞类型分布如表 1-2 所示。其中操作系统命令注入，占 27.12%。值得关注的还有缓冲区溢出、权限许可和访问控制等常见漏洞类型。

表 1-2 2018 年 6 月漏洞类型分布

类型	数量	比例
缓冲区溢出	12	6.78%
权限许可和访问控制	13	7.34%
信息泄露	2	1.13%
操作系统命令注入	48	27.12%
跨站请求伪造	6	3.39%
资源管理错误	2	1.13%
SQL 注入	2	1.13%
路径遍历	1	0.56%
跨站脚本	19	10.73%
未知	72	40.68%

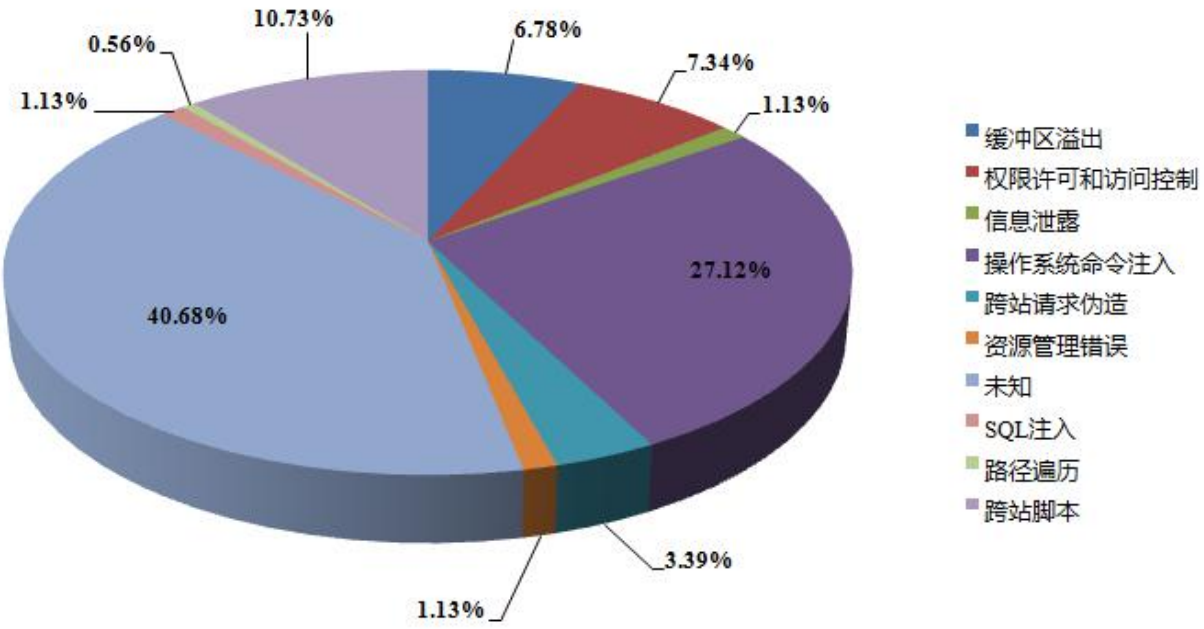

图 1-2 2018 年 6 月漏洞类型占比

三、 高危漏洞实例

(一) phpMyAdmin 远程代码执行漏洞

CVE 编号：CVE-2018-11235

CNNVD 编号：CNNVD-201806-1096

发布时间：2018-06

危险等级：☆☆☆☆

漏洞类型：远程代码执行

受影响软件：

phpMyAdmin 4.8.0

phpMyAdmin 4.8.1

漏洞描述：phpMyAdmin 是一套免费的、基于 Web 的 MySQL 数据库管理工具，方便的建立、修改、删除数据库及资料表。

该漏洞可以被攻击者利用来进行文件包含甚至进一步的代码执行攻击。漏洞点出现在 phpMyAdmin 重定向和加载页面的代码以及不合理的白名单页面测试。除以下情况，攻击者必须通过认证才能进行攻击：1.$cfg['AllowArbitraryServer'] = true:这个配置使得攻击者可以指定他控制的任意主机并且在 phpmyadmin 上执行代码。
2.$cfg['ServerDefault'] = 0:这个配置使得攻击者无须认证即可绕过登录并运行代码。

攻击者可以利用该漏洞远程执行恶意代码，危害系统安全。

修补建议：应用补丁，或者升级到 phpMyAdmin 4.8.2 或更高版本，补丁获取链接：

https://github.com/phpmyadmin/phpmyadmin/commit/7662d02939fb3cf6f0d9ec32ac664401dcfe7490

(二) Apache Storm 任意文件写漏洞

CVE 编号：CVE-2018-8008

CNNVD 编号：CNNVD-201806-318

发布时间：2018-06

危险等级：☆☆☆☆

漏洞类型：路径遍历

受影响软件：

Apache Group Storm <= 1.2.1

Apache Group Storm <= 1.0.6

Apache Group Storm 1.1.2

漏洞描述：Apache Storm 是一款免费、开源的分布式实时计算系统，可以轻松、可靠地处理无限数据流，可以与任何编程语言一起使用。

攻击者可以利用该漏洞通过精心制作的带有目录遍历文件名的压缩文档（zip，bzip2，tar，xz，war，cpio，7z 等），当文件名连接到目标提取目录时，最终会导致文件将解压在目标文件夹之外。

攻击者可以利用该漏洞获取敏感文件，危害系统安全。

修补建议：目前厂商已经发布了升级补丁，补丁获取链接：

https://lists.apache.org/thread.html/613b2fca8bcd0a3b12c0b763ea8f7cf62e422e9f79fce6cfa5b08a58@%3Cdev.storm.apache.org%3E

（三） PHP 拒绝服务漏洞

CVE 编号：CVE-2018-12882

CNNVD 编号：CNNVD-201806-1343

发布时间：2018-06

危险等级：☆☆☆☆

漏洞类型：拒绝服务

受影响软件：

PHP 7.2.x - 7.2.7

漏洞描述：PHP 是一种被广泛使用的脚本语言，用于基于 Web 的 CGI 程序，它可被安装在包括 Apache、IIS、Caudium、Netscape、iPlanet 和 OmniHTTPd 等多种 Web 服务器上。

该漏洞与 ext/exif/exif.c 文件的‘exif_read_from_impl’函数有关，是由于程序关闭了一个不应该关闭的流。易受攻击的代码可通过 PHP exif_read_data 函数访问。攻击者可以利用该漏洞造成拒绝服务攻击。

攻击者可以利用该漏洞造成拒绝服务攻击，危害系统安全。

修补建议：目前厂商已经发布了升级补丁，补丁获取链接：

https://bugs.php.net/bug.php?id=76409

(四) Joomla!本地文件包含漏洞

CVE 编号：CVE-2018-12712

CNNVD 编号：CNNVD-201806-1219

发布时间：2018-06

危险等级：☆☆☆

漏洞类型：文件包含

受影响软件：

Joomla! 2.5.0 - 3.8.8

漏洞描述：Joomla!是 Open SourceMatters 团队开发的一套开源的使用 PHP 语言和 MySQL 数据库的内容管理系统(CMS)，是网站的一个基础管理平台。可以在 Linux、Windows、MacOSX 等各种不同的平台上执行。

该漏洞与“class_exists”函数有关，该函数是检查类名是否有效，会将无效名称验证为有效，从而导致本地文件包含，导致信息泄露的风险。

攻击者可以利用该漏洞造成敏感信息泄露，甚至执行任意代码。

修补建议：升级到版本 3.8.9 或以上版本，版本链接：

https://downloads.joomla.org/

(五) NTP 缓冲区溢出漏洞

CVE 编号：CVE-2018-12327

CNNVD 编号：CNNVD-201806-1071

发布时间：2018-06

危险等级：☆☆

漏洞类型：缓冲区错误

受影响软件：

NTP 4.2.8p11

漏洞描述：NTP(Network Time Protocol)是一种使网络中计算机的时间同步的协议，ntpq 和 ntpdc 是其中的 NTP 状态的查询程序。

该漏洞与 ntpq 和 ntpdc 有关，攻击者可以利用该漏洞通过使用长字符串作为 IPv4 或 IPv6 命令行参数实现代码执行或提升到更高权限。

攻击者可以利用该漏洞导致代码执行，危害系统安全。

修补建议：目前厂商还没有提供补丁或者升级程序，厂商获取链接：

http://www.ntp.org/

四、 本月安全要闻

（一） 韩国最大虚拟币交易平台被黑，约 2 亿元资产被盗

据韩联社报道，韩国最大虚拟货币交易平台 Bithumb 遭黑客入侵，约 350 亿韩元(约合人民币 2.04 亿元)资产被盗。

据 Bithumb 介绍，公司于当地时间 19 日下午 11 时发现异常情况，于 20 日凌晨 1 时 30 分许采取限制存储措施后清点资产发现了平台被黑情况，随后于当天上午 9 时 40 分许向韩国网络振兴院(KISA)举报。

Bithumb 紧急通知，约 350 亿韩元的加密货币被盗，平台暂停交易和加密货币的存取服务。损失的部分将由公司赔偿，客户资产已转移到未接入互联网的外部存储设备。

Bithumb 相关人士表示，将对服务器进行优化升级，加强数据库安全防护，确保今后不再发生类似情况。

另外，Bithumb 被黑消息传出后，币价较前一交易日下滑 4.25%，其他虚拟货币也应声齐跌。

友情链接：http://hackernews.cc/archives/23346

（二） DNA 检测公司 MyHeritage 遭黑客入侵：9200 万账户泄露

北京时间 6 月 6 日早间消息，消费级家谱网站 MyHeritage 宣布，与该公司的 9200 万个帐户相关的电子邮件地址和密码信息被黑客窃取。

MyHeritage 表示，该公司的安全管理员收到一位研究人员发送的消息，后者在该公司外部的一个私有服务器上发现了一份名为《myheritage》的文件，里面包含了 9228 万个 MyHeritage 帐号的电子邮件地址和加密密码。

“没有证据表明文件中的数据被犯罪者利用。”该公司周一晚些时候在声明中说。

MyHeritage 允许用户制作家谱、搜索历史记录并寻找潜在的亲人。该公司 2003 年创办于以色列，2016 年推出了 MyHeritage DNA，用户只要发送一份唾液样本即可进行基因检测。该网站目前拥有 9600 万用户，其中有 140 万曾经接受过基因检测。

据 Heritage 介绍，该漏洞发生在 2017 年 10 月 26 日，受影响的用户都是在那一天之前注册的。该公司还表示，他们并没有存储用户的密码，所有密码都经过所谓的单项散列方式进行加密，不同用户的数据需要使用不同的密钥才能访问。

但在之前的黑客事件中，这类机制曾经遭到破解，从而转换出密码。倘若如此，黑客便可获在登录用户帐号后获取其个人信息，包括家庭成员的身份。但即使黑客能够进入用户帐号，也不太可能轻易获取原始基因信息，因为想要下载这些内容，需要通过电子邮件进行确认。

该公司在声明中强调，DNA 数据存储在“隔离的系统上，与保存电子邮件的系统相互分离，其中包含额外的安全层。”

MyHeritage 已经组建了全天候支持团队，为受影响的用户提供帮助。该公司还计划聘请独立网络安全公司调查此事，并有可能加强安全措施。与此同时，他们也建议用户更改密码。

随着消费级 DNA 测试发展成为一个 9900 万美元的行业，关于用户私密数据的安全性问题也引发越来越多的关注。在调查者通过某家谱网站追踪到“金州杀手案”嫌疑人后，关于 DNA 数据的隐私担忧也大幅提升。

友情链接：http://hackernews.cc/archives/23241

（三） 美国大数据公司失误泄露 2TB 隐私信息：涉 2.3 亿人

据 Wired 报道，本月初曝光的市场和数据汇总公司 Exactis 服务器信息暴露的事情经调查为实。Exactis 采集了大约 3.4 亿条记录，大小 2TB，可能涵盖 2.3 亿人，几乎是全美的上网人口。Exactis 此次的信息泄露并不是黑客撞库引起或者其它恶意攻击，而是他们自己的服务器没有防火墙加密，直接暴露在公共的数据库查找范围内。

最早发现的安全研究员 Vinny Troia 称，他想搜索的所有人的资料都可以在泄露数据中找到，《连线》的记者给了 10 个名字，最后准确返回 6 个结果。

虽然上述信息中不包含信用卡号、社会保障号码等敏感的金融信息，但是隐私深度却超乎想象，包括一个人是否吸烟，他们的宗教信仰，他们是否养狗或养猫，以及各种兴趣，如潜水和大码服装，这几乎可以帮助构建一个人的几乎完整“社会肖像”。

目前，Exactis 已经对数据进行了加密防护。在其官网，Exactis 号称服务 2.18 亿独立用户，总计手机了超过 35 亿条商业、消费者和数字信息。

友情链接：https://www.cnbeta.com/articles/tech/740975.htm

（四） 警惕：美国出现黑客盗取并兜售幼儿个人信息

据美国“侨报网”6 月 27 日报道，盗窃身份的网络黑客现在已将黑手伸向了持有社会安全号码(SSN)的年幼孩子——甚至包括新生婴儿，因为这些孩子从来没有购买过任何东西，这意味着他们有一个“完美”的信用记录。

而黑客在窃取了这些拥有“完美”信用记录的身份信息后，会在黑市网站上进行兜售，并会向买家解释如何使用这些信息伪造欺诈性税务记录或申请信用卡而不被抓获。不幸的是，当这些孩子长大后，他们可能会发现自己的信用出了问题，但纠正信用历史问题或欺诈性购买等将是非常困难或根本不可能做到的事情。

纽约医疗保健公司 Cynerio 首席执行官里尔曼(Leon Lerman)指出，该公司研究人员已发现，在“黑暗网站”上有一个复杂的市场，被盗数据可通过一定的渠道分销给最终用户，而黑客作为黑市价值链的顶端，已将大量原始患者数据出售给买家。而这对公众尤其是孩子的家长也提出了警示。

对此，他表示，为了避免个人信息外泄，除非绝对需要，否则应尽量保护个人信息的安全。一旦有孩子信息被盗，家长必须为孩子注册新的社安号。

BTB 安全管理公司合伙人施乐西特(Ron Schlecht)也指出，黑客之所以窃取儿童数据，还因为它可以与其他数据相结合。例如，由于 SSN 和出生日期数据是真实的，黑客可使用伪造的名称和地址建立信用记录，而这是一种将真实信息和虚假信息结合起来的欺诈行为。

对此，消费及商业专家建议，孩子家长最好定期检查孩子们的信用记录。黑客对婴幼儿下手主要因为很多家长多年来疏于对孩子信用历史的检查。若孩子信用被滥用，可能需要他们靠年份积累来补救和恢复他们的身份和名誉，在极端情况下，他们可能需要获得一个新的社安号。此外，父母还应注重保护孩子的身份信息，切勿随意向外透露，包括学校、医院等。

友情链接：https://www.cnbeta.com/articles/tech/741169.htm

（五） 航旅纵横“选座社交”陷隐私泄露争议

航旅类 App 航旅纵横因最近上线的“虚拟客舱”功能引发争议。通过这个功能，用户可以查看同舱乘客的历史飞行地点及频率等信息，还可以与同客舱的乘客进行私聊。有网友担心，该功能存在隐私泄露隐患。“目前已将虚拟个人主页设为默认关闭状态，产品后续将会进一步改进”，航旅纵横就此致歉并回应。

此功能是目前正在部分航线测试的新功能，展示的不是个人的真实身份信息，头像、昵称、标签等均为可编辑的信息，标签由用户自行添加，热力图进行了虚化处理。

有专家认为，目前越来越多的功能性软件增加了社交功能，但“捆绑”的个人信息也会给用户带来安全隐患，运营商在相关类似功能时需更加谨慎。

苹果 App Store 的软件历史更新记录显示，航旅纵横 App 在今年 6 月 5 日的软件更新中，加入了“可查看同机人主页”的信息，将其形容为“志同道合好结伴”。

6 月 11 日，有网友通过“航空物语”微信公众号发表文章称，自己在使用航旅纵横软件查看座位信息时，发现可查看同航班乘客个人主页，信息包括对方座位号、头像、昵称或姓名、职业、设置的标签以及热力图，还可进行私聊。

“通过这个功能，我可对照着飞机上的乘客本人查看他信息、通过热力图分析他的行为轨迹，感觉大家都跟透明人一样，我这么被人盯着，也很不舒服。”这位网友称，找了很久没找到关闭个人主页的按钮。

有网友质疑称，航旅纵横作为一个航旅类软件，向用户提供航班查询、值机选座等服务，掌握着大量用户的飞行数据等隐私信息。虚拟个人主页通过飞行热力图可查看个人历史飞行地点及频率，标签上的星座、职业信息等也涉嫌泄露个人隐私，而航旅纵横在未经用户同意的情况下将这些信息进行了公开。

6 月 11 日，航旅纵横通过官方微信公众号发文回应称，“虚拟客舱”功能设计的初衷，就是因为听到了大量用户的呼声，“为了帮助大家开启有温度的飞行”。

在选座入口，用户可以进入开启一键群聊模式，与同机舱的乘客聊天。新京报记者体验发现，用户选择座位后，聊天界面就会自动弹出相关信息：“我刚刚预约了座位 xx……期待坐在邻座的你哦。”

当用户点击已被选择的座位，则可以查看相关用户的个人主页信息，包括头像、标签及飞行热力图等，还可以与其进行私聊。

航旅纵横对此解释称，“如果你有特别需要帮助的，比如换个座位、寻求同航班的人的帮助等等……可以点击他的个人页面进行私聊。”内容中强调，通过虚拟客舱功能，用户可以搭建起与同客舱乘客交流的桥梁。

航旅纵横一工作人员当天接受新京报记者采访时表示，航旅纵横目前用户量超过 5000 万，虚拟客舱是近期航旅纵横正在部分航线测试的新功能，自上周开始测试，核心思路是想探索当机舱中的用户都在线的情况下出行服务能够有哪些创新，提升之前实现效率较低或无法满足的需求，比如很快我们会上线一键换座的功能，通过用户的线上沟通，解决用户只能选择在机上沟通换座的尴尬。

“这个功能并不是要做社交，而是希望探索用户在线模式下的服务创新可能。”该工作人员称，而个人主页的标签功能展示的不是个人的真实身份信息，均为头像、昵称、标签等可编辑的信息，标签由用户自行添加，热力图进行了虚化处理，整个个人主页用户可根据自己的意愿自行选择开启或者关闭，目前已经默认关闭状态。

该工作人员表示，个人主页信息默认关闭后，私聊不会涉及用户隐私的问题。

阚志刚表示，目前，中国对于个人隐私的界定不是很清晰，从专业的法律角度来说个人隐私包括身份证号、家庭住址等敏感信息，但同机人信息、飞行热力图、标签等可以算为法律规定中的灰色地带，不能算严格意义的个人隐私，计算机安全条例对于个人隐私不是非常明晰，建议在航旅纵横软件主页声明中主动告知用户如何使用、自主选择关闭与否，保障用户的知情权和选择权。

目前越来越多的应用软件增加了社交功能，从软件设计和运营来说是为了增加用户的黏性，初衷可能是好的，但只考虑到好的社交方面，没有考虑到泄露了一些用户信息会给用户带来隐藏的安全隐患，应该双面去理解。

友情链接：http://www.sohu.com/a/235632332_786964